

# TP Service sur réseaux N°5 - MMI1 - Semestre 2

## Introduction

Ce TP propose la mise en oeuvre de filtrage. Le réseau que nous allons étudier est constitué d'une zone privée, que nous pouvons comparer au réseau d'une petite entreprise. Un ISP fournit un routeur, sur lequel sont branchés les équipements du client.

Nous avons également une zone simulant un accès internet composée d'un serveur DNS et d'un serveur web, et enfin un PC en accès distant qui a la particularité d'avoir une IP publique.

L'entreprise souhaite protéger son réseau vis à vis des menaces extérieures et pour se faire, elle installe un firewall entre le routeur du provider et son propre réseau interne.

Afin de simplifier la configuration des équipements nous allons nous aider d'un outil open source qui s'appelle Firewall Builder. Ce logiciel permet de définir des règles de manières graphiques puis de les compiler en vue de les utiliser sur différents firewall possible. Nous allons donc créer les règles sur cet outil, puis effectuer un copier/coller dans le firewall de Packet Tracer.

## Travaux préliminaires

### Installation de Firewall Builder

1. Ouvrez Firefox depuis le menu, et authentifiez vous sur le Firewall de l'IUT.
2. Ouvrez le menu de Linux Mint et exécutez Konsole, puis exécutez les commandes suivantes :

```
utilisateur-VirtualBox: >sudo apt-get update
utilisateur-VirtualBox: >sudo apt-get install -y fwbuilder
```

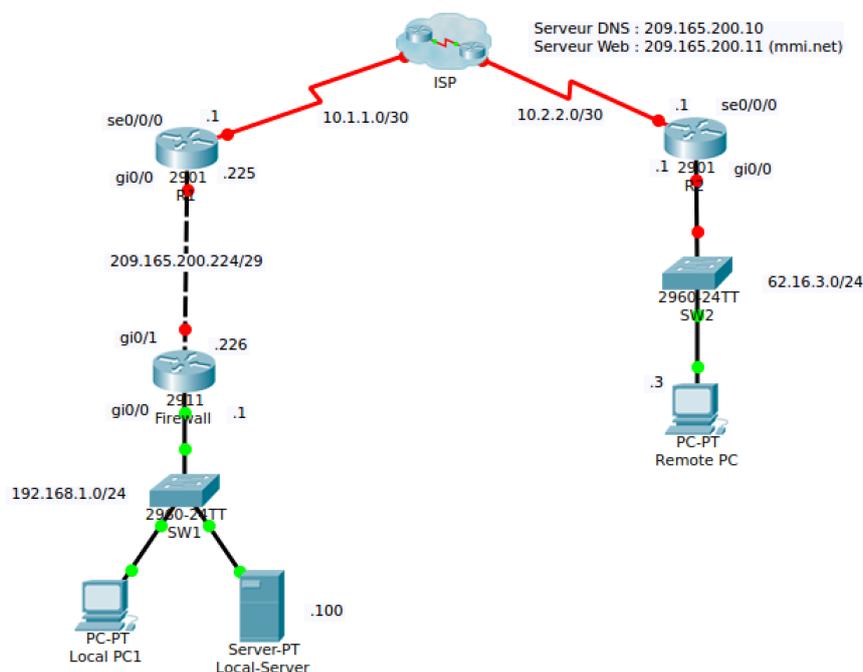
3. Une fois l'installation effectuée, chargez le fichier de base du firewall à l'adresse suivante :

<http://www.akatone.com/MMI/s2-tp5-ssr.fwb>

Firefox vous propose d'ouvrir ce fichier directement dans Firewall Builder, faites donc ainsi. A présent, laissez pour le moment firewall builder de côté. Nous allons tout d'abord finir la configuration du réseau.

### Construction du réseau

1. Téléchargez le réseau à l'adresse suivante : <http://www.akatone.com/MMI/s2-tp5-ssr.pkt>
2. Ouvrez Packet Tracer et chargez le fichier que vous venez de télécharger. Le réseau est pré-configuré. Complétez-le en répondant aux questions ci-dessous, en fonction du schéma.



## R1

1. Configurez les interfaces de R1 en suivant les indications du schéma.
2. Configurez la route par défaut.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 Serial0/0/0
```

## R2

1. Configurez les interfaces de R2 en suivant les indications du schéma.
2. Configurez la route par défaut.

## Firewall

1. Configurez la route par défaut.
2. Configurez le NAT :

```
Firewall(config)#interface gi0/0
Firewall(config-if)#ip nat inside
Firewall(config-if)#exit
Firewall(config)#interface gi0/1
Firewall(config-if)#ip nat outside
Firewall(config-if)#exit
Firewall(config)#ip nat pool MYNATPOOL 209.165.200.226
209.165.200.226 netmask 255.255.255.248
Firewall(config)#ip nat inside source list 7 interface gi 0/1
overload
Firewall(config)#access-list 7 permit 192.168.1.0 0.0.0.255
```

## Vérifications

Placez une croix à l'endroit approprié dans les tableaux ci-dessous.

### Note

Vous pouvez vérifier l'état du NAT grâce à la commande *show ip nat translation*.

1. Depuis le Local PC-1 pingez 209.165.200.11

	Ping OK	Ping No OK
Résultat		

2. Depuis le Local PC-1 pingez 62.16.3.3

	Ping OK	Ping No OK
Résultat		

3. Depuis le Remote PC pingez 209.165.200.11

	Ping OK	Ping No OK
Résultat		

4. Depuis le Remote PC pingez 192.168.1.100

	Ping OK	Ping No OK
Résultat		

5. Depuis le Local PC-1 ouvrez l'onglet « desktop » et affichez la page <http://mmi.net>

	Ping OK	Ping No OK
Résultat		

6. Depuis le Remote PC ouvrez l'onglet « desktop » et affichez la page <http://mmi.net>

	OK	No OK
Résultat		

7. Depuis le Remote PC ouvrez l'onglet « desktop » et affichez la page <http://192.168.1.100>

	OK	No OK
Résultat		

8. Pouvez vous expliquer pourquoi certaines opérations ne fonctionnent pas ?

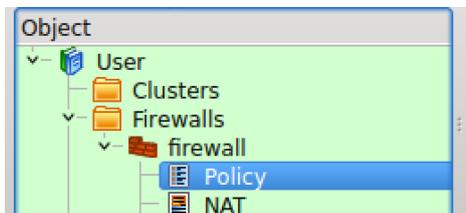
## Filtrage simple

Maintenant que notre réseau est fonctionnel, il convient maintenant de le protéger. Dans Firewall Builder, compilez  les règles, puis cliquez sur  afin de copier/coller la configuration dans le Firewall (en mode config, bien entendu).

Par défaut, le firewall filtre (presque) tout. Nous allons ajouter les services minimums.

### ICMP

Afin de diagnostiquer notre infrastructure, nous allons permettre l'usage des ping, traceroute etc... sur toutes les interfaces. Cliquez sur l'icone « Policy » afin d'afficher les règles.



1. Remplissez le tableau de règles correspondant :

Source	Destination	Service	Interface	Direction	Action

2. Implémentez la règle (c'est à dire compilez, puis copier/collez le résultat dans le firewall de Packet Tracer).  
3. Testez.

## Accès au Web

1. Quels sont les services nécessaires à ajouter pour accéder au Web ?

-

2. Remplissez le tableau de règles correspondant

<b>Note</b>	Pour vous aider dans l'établissement de vos règles, n'oubliez pas que TCP est un protocole connecté, vous avez un objet 'ESTABLISHED' qui vous permettra de matcher les paquets faisant partie d'une connection.
-------------	--

Source	Destination	Service	Interface	Direction	Action

3. Implémentez les règles

4. Testez en ouvrant depuis le PC Local l'adresse <http://mmi.net>

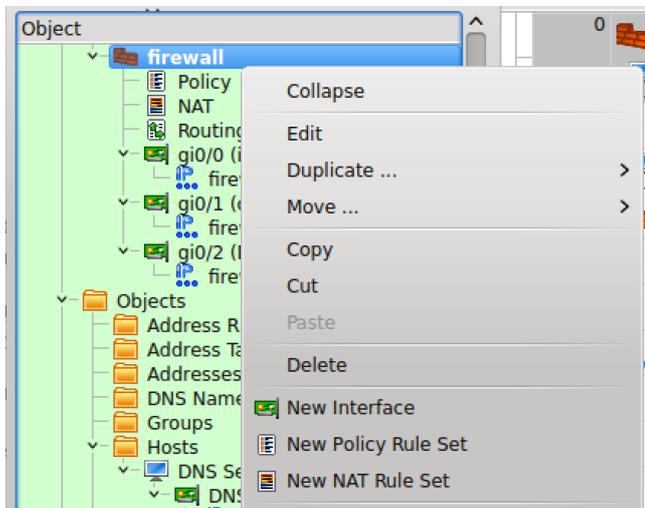
## DMZ

Une configuration réseau classique comporte généralement une ou plusieurs DMZ. Les serveurs placés en DMZ ont la particularité d'être accessible depuis l'extérieur et l'intérieur. On y abrite par exemple un serveur VPN (pour un accès distant sécurisé), un portail web ou un serveur d'authentification etc.

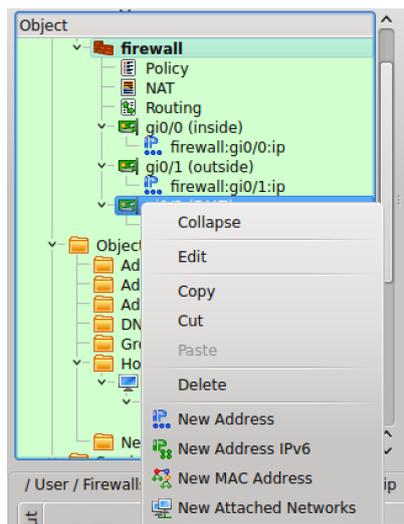
### Configuration du firewall

Pour créer une DMZ, nous allons tout d'abord ajouter une interface à notre firewall dans Firewall Builder.

1. Clic droit de la souris sur l'icône du firewall et choisissez l'option « New Interface ».

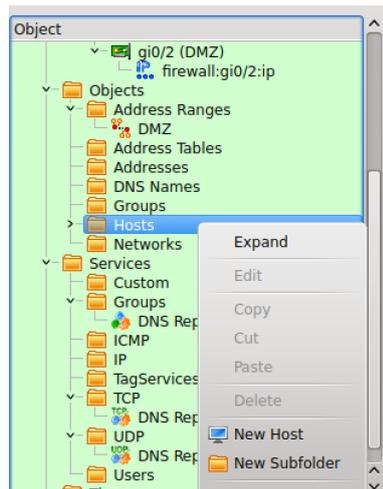


2. Dans le champ name, appelez la nouvelle interface « gi0/2 », label = « DMZ ».
3. Clic droit sur l'interface que vous venez de créer, et choisissez l'option « New Address ».

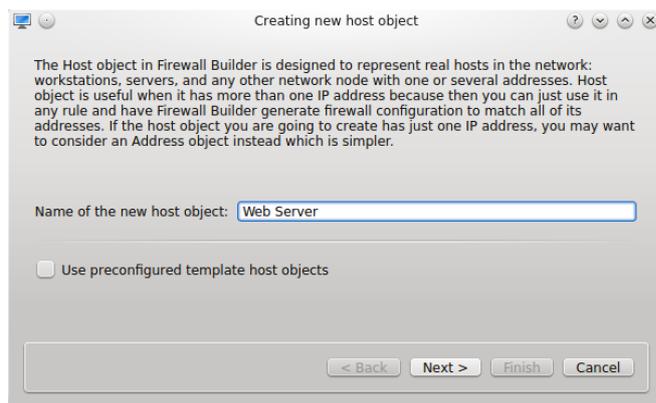


Ensuite nous allons créer un objet représentant un serveur en DMZ.

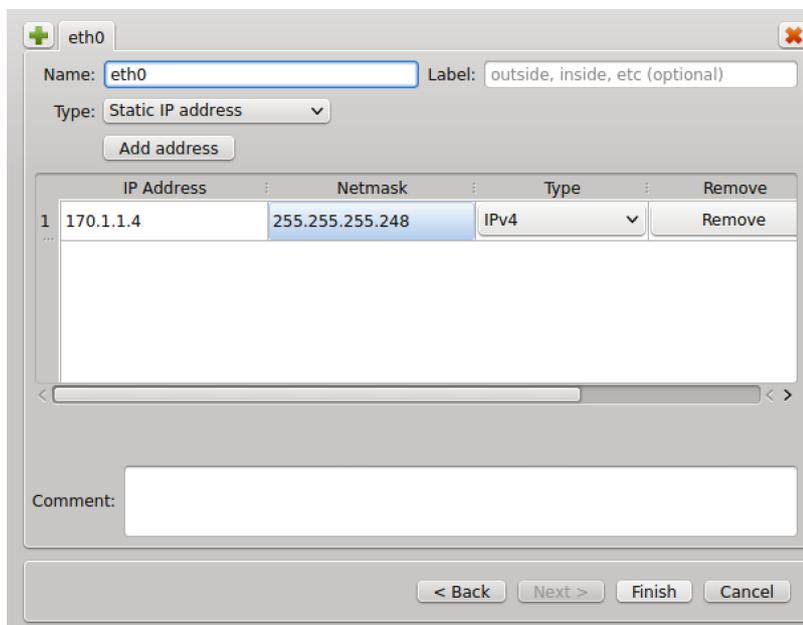
4. Clic droit sur la zone des objets/Hosts et choisissez 'New host'.



5. Puis, renseignez le nom du serveur comme ceci :



6. Cliquez sur 'Next' 2 fois. Puis remplissez les informations relatives à l'adresse IP comme ceci :



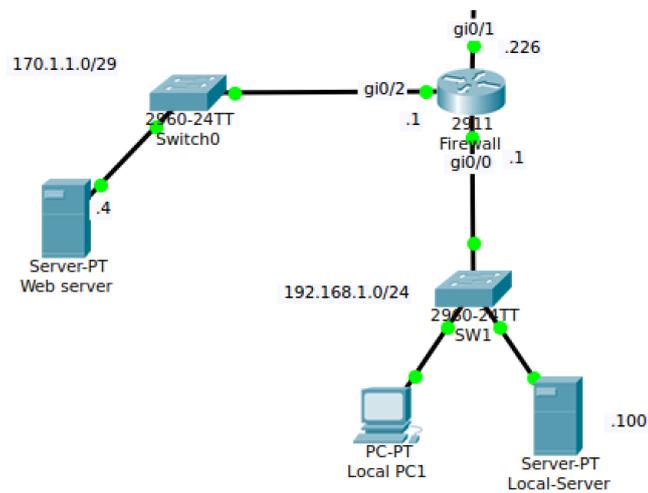
7. Et enfin cliquez sur 'Finish'.

8. Maintenant que les objets utiles sont créés, vous pouvez définir les règles sur le firewall permettant l'accès à un serveur web placé en DMZ.

Source	Destination	Service	Interface	Direction	Action

### Implémentation

Côté Packet Tracer, il faut maintenant créer l'architecture de la DMZ, tel que définie sur le schéma ci-dessous :



Testez à présent votre configuration en tentant de vous connecter à l'adresse <http://extranet.mmi.net> depuis à la fois un PC local mais également depuis le PC distant.